Department of Energy & Climate Change

Smart Metering Implementation Programme:

Device Assurance Framework User Guide

August 2015

© Crown copyright 2015

URN: 15D/419

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence.

To view this licence, visit www.nationalarchives.gov.uk/doc/open-government-licence/
or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU,
or email: psi@nationalarchives.gsi.gov.uk.

Any enquiries regarding this publication should be sent to smartmetering@decc.gsi.gov.uk.

Contents

Introduction....4
What is device assurance?....4
The Device Assurance Framework....6
Formal provisions supporting Device Functionality....6
Formal provisions supporting Device Interoperability....6
Emerging informal device assurance services and tools....8
What does the testing journey for assured devices look like?....9
Summary of Key Findings from Stakeholder Engagement....10

Introduction

The Device Assurance Framework (DAF) has been developed to support the delivery of fully functional and interoperable smart devices. The formal regulatory provisions underpinning the DAF are complemented by industry-led assurance initiatives. This guide is intended to provide clarity on both the formal regulated elements of the framework and the informal industry-led provisions that have emerged more recently. It comprises the following sections:

- An introduction to device assurance;
- An explanation of the formal regulated provisions underpinning the DAF;
- An outline of the informal industry-led arrangements that are emerging; and
- A summary of the key findings of the stakeholder engagement completed to assess the response of industry parties to the overall Device Assurance framework.

What is device assurance?

Device assurance activities are undertaken to provide confidence that smart metering equipment will perform as expected when it is installed, both in isolation and in association with other parts of the system (including with other in-home equipment and the DCC). We have identified two key aspects of devices that require assurance: Device Functionality; and Device Interoperability (as illustrated in Figure 1).

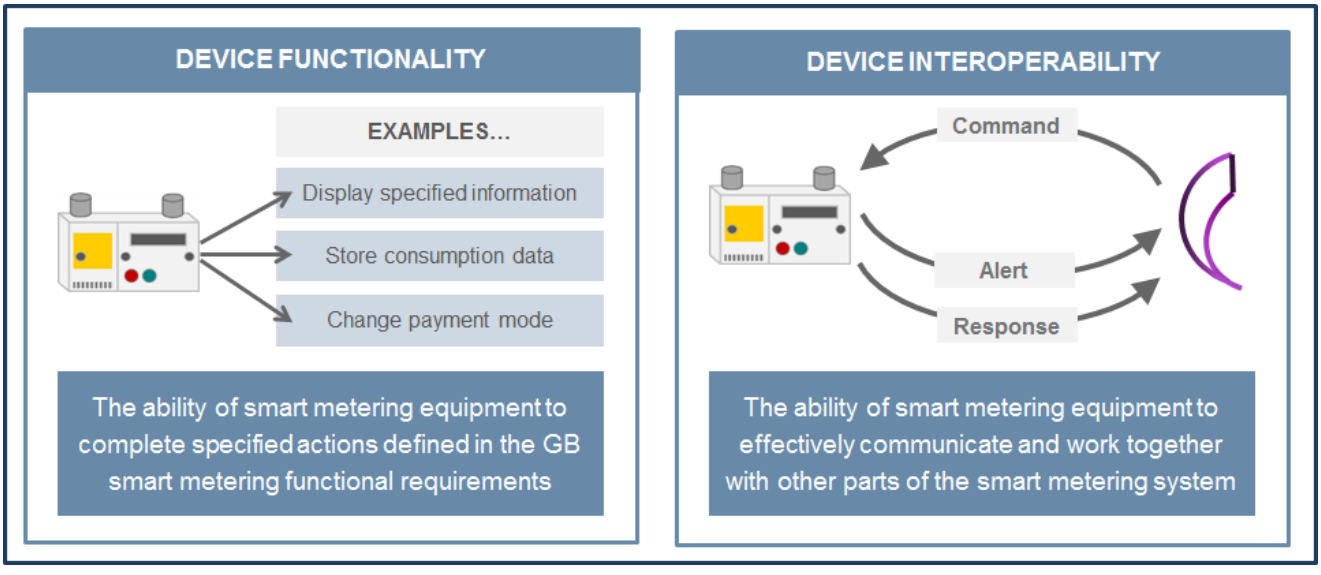
DEVICE FUNCTIONALITY
EXAMPLES...
Display specified information
Store consumption data
Change payment mode
The ability of smart metering equipment to complete specified actions defined in the GB smart metering functional requirements
DEVICE INTEROPERABILITY
Command
Alert
Response
The ability of smart metering equipment to effectively communicate and work together with other parts of the smart metering system

Figure 1: An overview of the components comprising Device Assurance

From a consumer perspective fully functional and interoperable smart devices will help ensure that they have access to accurate and reliable data, increasing their ability to make informed decisions on their energy consumption. In addition, it will reduce the risk of devices needing to be replaced on change of supplier (COS), which could cause inconvenience and reduced confidence in smart meters.

From the point of view of DCC Users (suppliers, network operators and other users), fully functional and interoperable devices will support the exchange of smart meter data and messages to support related business processes; for example, change of supplier, change of

tenancy, etc. In the event that the functionality and interoperability of devices is compromised, this ability will be limited; significantly reducing the potential benefits of the smart meter roll out.

Device interchangeability refers to the ability of devices connected to the Home Area Network (HAN) to function in a consistent way regardless of type and combination installed. Figure 2 provides a simplified representation of the concept of device interchangeability, illustrating that it may be particularly relevant following COS. For example if a device needs to be replaced following a COS, device interchangeability would ensure that all of the devices on the HAN continue to work with each other; even though they may have been produced by different manufacturers.

While device interchangeability is not specifically referenced in the DAF, in practice a consistent interpretation of device functionality (as described in SMETS), compliance with the GBCS and ZigBee certification should provide interchangeable devices.

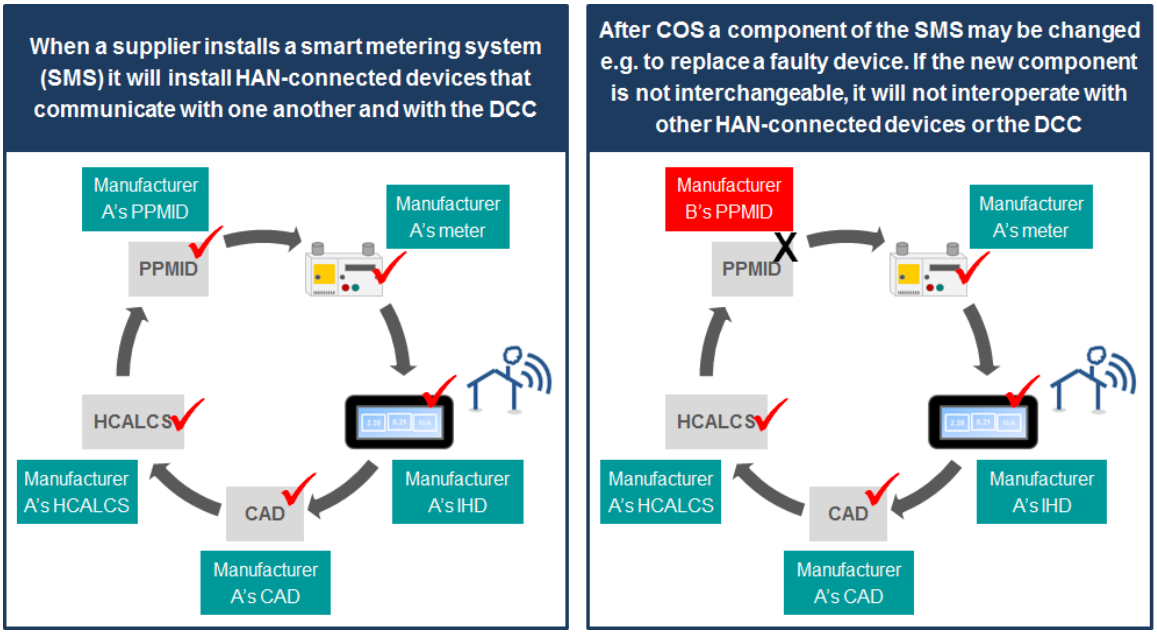
When a supplier installs a smart metering system (SMS) it will install HAN-connected devices that communicate with one another and with the DCC
Manufacturer A's PPMID
PPMID
Manufacturer A's meter
HCALCS
Manufacturer A's HCALCS
CAD
Manufacturer A's IHD
Manufacturer A's CAD
After COS a component of the SMS may be changed e.g. to replace a faulty device. If the new component is not interchangeable, it will not interoperate with other HAN-connected devices or the DCC
Manufacturer B's PPMID
X
PPMID
Manufacturer A's meter
HCALCS
Manufacturer A's HCALCS
CAD
Manufacturer A's IHD
Manufacturer A's CAD

Figure 2: An overview of the concept of interchangeability

The Device Assurance Framework

Figure 3 provides a high level overview of the formal regulatory elements of the DAF. The Energy Act 2008 included provisions to establish the formal regulatory tools for smart metering, including device assurance provisions.

The DCC licence, the gas and electricity supply licences, and the SEC contain high level device assurance provisions, including obligations to:

- Ensure installed devices are compliant with the SMETS/ CHTS/ GBCS and retain evidence of this;
- Test devices for DCC interoperability and retain evidence of this;
- Ensure the end-to-end system is secure;
- Establish a Certified Product List (CPL).

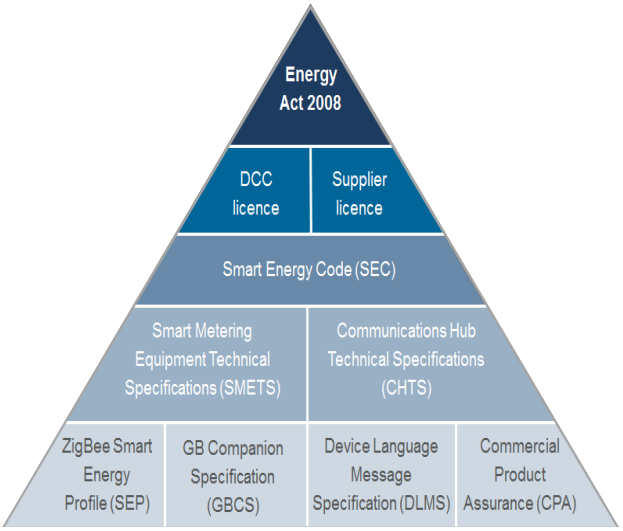
Energy Act 2008
DCC licence
Supplier licence
Smart Energy Code (SEC)
Smart Metering Equipment Technical Specifications (SMETS)
Communications Hub Technical Specifications (CHTS)
ZigBee Smart Energy Profile (SEP)
GB Companion Specification (GBCS)
Device Language Message Specification (DLMS)
Commercial Product Assurance (CPA)

Figure 3: DAF hierarchy

The detailed Device Functionality and Device Interoperability requirements are contained in the Smart Metering Equipment Technical Specifications (SMETS) and Communications Hub Technical Specifications (CHTS), which in turn require compliance with the GB Companion Specification (GBCS), Commercial Product Assurance (CPA) Security Characteristics, Device Language Message specification (DLMS) Companion Specification for Energy Metering (COSEM) and ZigBee Smart Energy Profile (SEP). Figure 4 describes the DAF pictorially (in addition to existing and informal assurance provisions).

Formal provisions supporting Device Functionality

As illustrated in Figure 4, the SMETS and CHTS describe the Device Functionality requirements for Gas Smart Metering Equipment (GSME), Electricity Smart Metering Equipment (ESME), In Home Displays (IHDs), Communications Hubs (CHs), the Pre-Payment Interface Devices (PPMIDs) and HAN-Connected Auxiliary Load Control Switches (HCALCSs). The SMETS and CHTS also explicitly require testing of devices against the technical specifications (the precise nature of the testing is not defined). This is complemented by SEC obligations that require parties to retain and to provide on request, evidence of compliance with the SMETS and CHTS.

The CPA Security Characteristics provide further definition of the security provisions provided in the SMETS and CHTS; parties are required to comply with the Security Characteristic and to obtain compliance certification from CESG. While the GBCS is not explicit about functionality requirements for smart devices, it includes some implicit functionality assumptions given the associated requirements related to communications with the DCC and its systems. Once again parties are required to undertake testing and retain evidence of compliance with the GBCS.

Formal provisions supporting Device Interoperability

The GBCS is the foundation upon which interoperability provisions for the smart metering system in GB are based; as noted above the SMETS and CHTS place obligations on suppliers and the DCC respectively to ensure that devices meet the GBCS requirements. The GBCS is based on open international standards, principally ZigBee SEP and DLMS COSEM:

- ZigBee SEP includes provisions that support (1) interoperability of devices via the HAN and (2) the basis for communications of end-to-end messages between devices and the

CH ("tunnelling"). The details of what needs to be certified for each device type is set out in the ZigBee SEP standard and GBCS[1]. In addition some aspects of ZigBee SEP are used for gas meter E2E messages ('GBZ' messages in GBCS) but these are not certified by the ZigBee Alliance.

- DLMS COSEM includes a series of provisions to support end-to-end message security and end-to-end message structures across all devices, and the data model for the electricity meter only. The SMETS places an obligation to obtain certification of device compliance with the DLMS COSEM specifications from the DLMS User Association for the electricity meter only.

The original intent of GBCS was that it would predominantly reference the ZigBee SEP and DLMS COSEM standards to ensure interoperability. However, as the security models developed it became apparent that significantly more bespoke content would be required to provide an interoperable and secure solution. ZigBee SEP and DLMS COSEM still underpin interoperability but on their own do not provide the full answer. It is difficult to ascribe a percentage to what proportion of Device Interoperability ZigBee and DLMS certfication provide but Figure 5 shows that they touch most aspects of GBCS.

In addition to the GBCS requirements, the suppliers (SEC Section F4) and DCC (CHTS) are

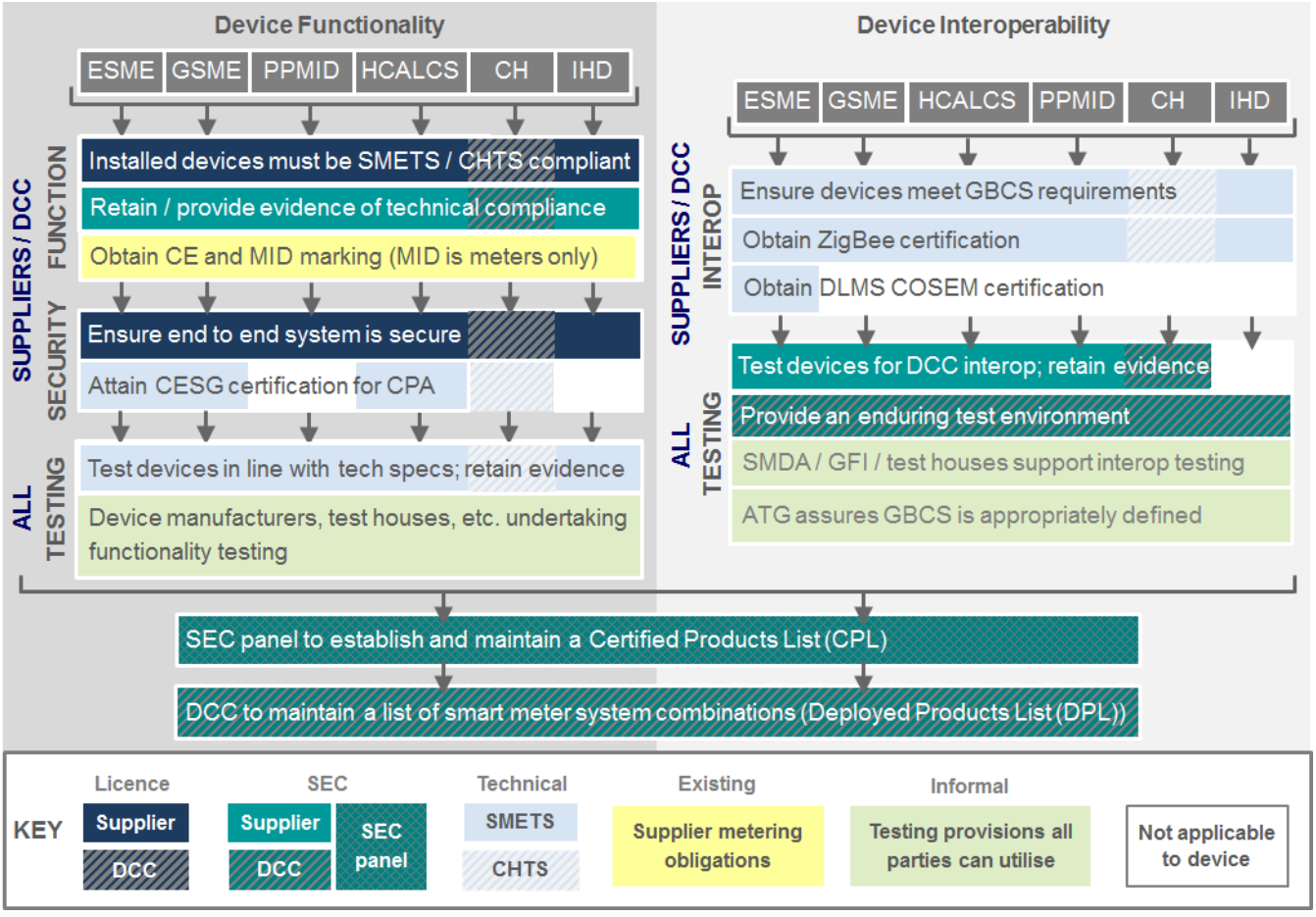

Figure 4: The overarching formal and informal Device Assurance framework

required to ensure that their devices are interoperable with DCC Systems; parties are required to undertake testing and retain evidence to this effect (the precise nature of the testing is not defined, however the DCC is required to provide a test environment to support this activity).

[1] GBCS sets out the 'optional' ZigBee SEP features that are mandatory for devices deployed as part of GB roll out.

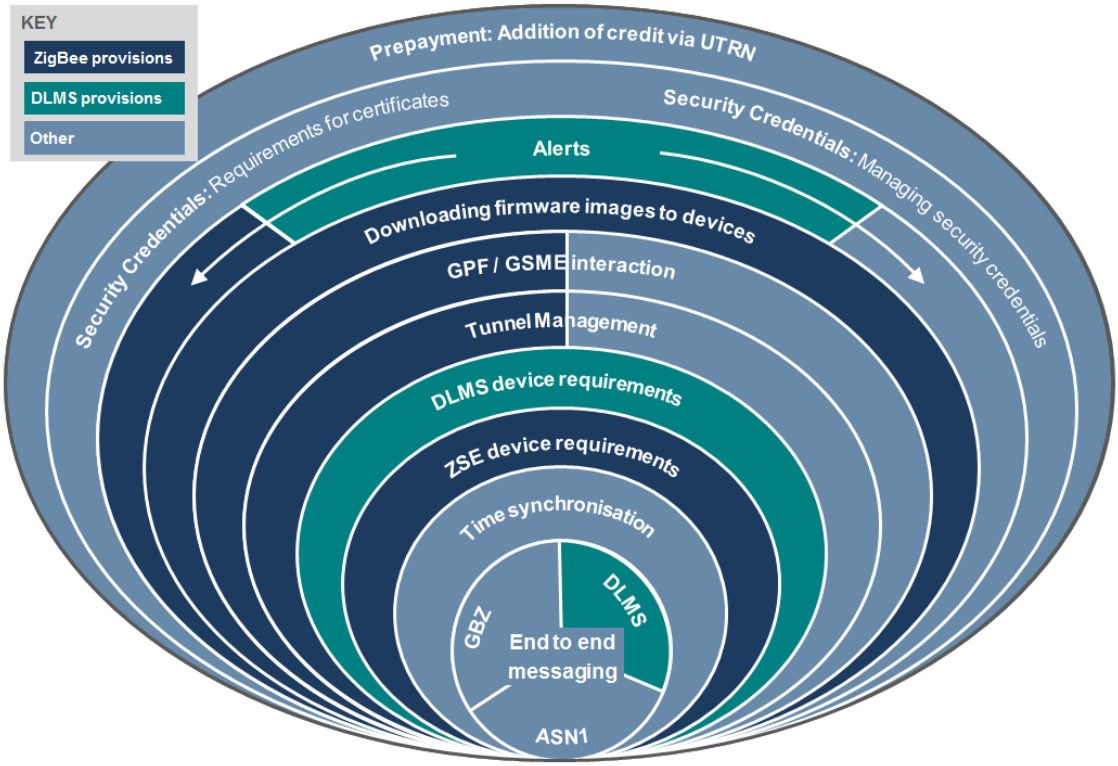

Figure 5: GBCS, ZigBee SEP and DLMS interoperability interactions

Emerging informal device assurance services and tools

A number of informal testing arrangements have emerged in recent months, including:

- **Services:** Includes the Smart Meter Device Assurance (SMDA) arrangements and third party test houses offering SMDA-like services and SMETS functionality testing; and
- **Tools:** Includes GBCS Integrated Testing (GIT) for Industry (GFI) (building on ATG).

Smart Meter Device Assurance

SMDA was initiated by Energy UK, BEAMA, the Energy and Utilities Alliance (EUA), and the Community of Meter Asset Providers (CMAP) as a way of providing energy suppliers a means of testing compliance with their GBCS and DCC interoperability obligations. The scheme will be self-governed, voluntary, independent and available to all industry parties (DNOs are considering getting involved).

SMDA will establish a central regime for interoperability and interchangeability testing, which they define as:

- **Interoperability:** The ability of devices to interface and operate with the DCC including the receipt and interpretation of commands and the connection of devices to CHs.
- **Interchangeability:** The compatibility of SMETS compliant devices with devices produced by different manufacturers including the ability to send, receive and interpret HAN messages, and securely connect Type one and Type two devices.

Gemserv has been appointed to the role of Scheme Operator (SO) following a competitive tender process. As SMDA SO, Gemserv will be responsible for defining common test scenarios, writing test specifications, setting testing charges and appointing test houses to provide a consistent, competitive testing service to users. It is expected that SMDA test houses will utilise remote DCC test environments with all DCC CH variants.

ATG and GBCS Integration Testing for Industry ('GIT' for Industry or GFI)

The DCC initiated ATG to identify any defects in the GBCS via automated testing. The goal of the ATG is to provide an increased level of confidence in GBCS end-to-end smart metering messages prior to the commencement of SIT.

The DCC is now working to extend ATG to enhance the confidence of industry parties with respect to the interoperability of smart meters with DCC systems, this is known as GFI. GFI will provide SEC parties, meter manufacturers and test houses with a tool (USB dongle) containing the GBCS end-to-end messages used in ATG (i.e. this will not include HAN only messages including between the gas proxy function and the GSME). The DCC anticipates that GFI will be made available to all interested parties in summer 2015.

What does the testing journey for assured devices look like?

Figure 8 below presents an overview of a testing journey. The diagram is intended to illustrate: the stages of testing that a device will go through including the focus of that stage and the "tools" used to support the stage (e.g. SMDA); our current best view on phasing associated with each stage; and which parties are likely to undertake the activity. The diagram highlights that different parties may adopt different sequences to attain assurance and that there is no predefined order or specified dates for certain tests as many of the testing services overlap.

A device can only be enrolled with DCC if it is on CPL. The CPL entry will detail the hardware and firmware versions. If the firmware of a deployed device needs to change then the CPL needs to be updated before any deployed devices are upgraded. It is the responsibility of the supplier to determine whether recertification under ZigBee, DLMS and CPA is required for any change in firmware.

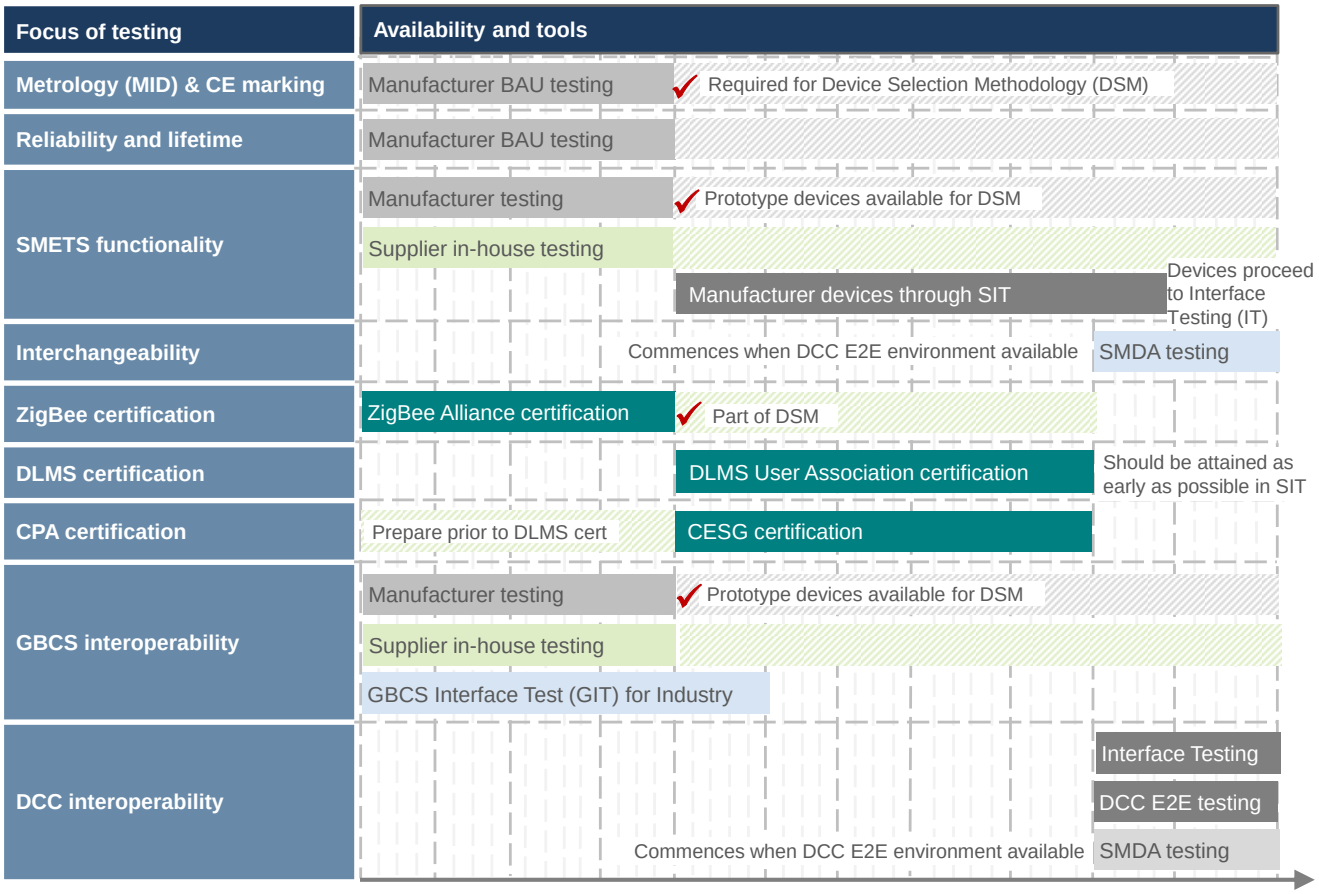

Figure 6: Illustration of an assurance journey

Summary of Key Findings from Stakeholder Engagement

Figure 7 below provides a summary of the key findings from the stakeholder engagement which involved discussions with seven energy suppliers, two meter manufacturers, two MAPs, DCC, the SMDA scheme operator and two test houses on device assurance.

Functionality testing	Interoperability testing	Other areas of testing
▪ Manufacturers and some suppliers intend to carry out functionality testing ▪ Some suppliers have established test labs for regulatory and business process testing ▪ Test cases are being generated for each requirement in the SMETS, CHTS and GBCS ▪ SMDA does not intend to explicitly provide functional testing ▪ Third party test houses intend to offer functionality testing to manufacturers and suppliers	▪ Most suppliers intend to use SMDA while others also intend to complete in-house testing for regulatory compliance and business processes ▪ Some suppliers and manufacturers intend to use DCC test environment ▪ Manufacturers intend to use the GIT for Industry tool ▪ The DCC test environment is critical to end-to-end interoperability testing	▪ SMDA intends to offer interchangeability testing ▪ Some suppliers also intend to undertake interchangeability testing ▪ Manufacturers and MAPs intend to undertake reliability and lifetime testing ▪ Manufacturers intend to undertake MID / CE testing ▪ Suppliers and manufacturers intend to undertake negative testing

Test scenarios	Sequencing	Dependencies
▪ No evidence of common test scenarios between stakeholders ▪ Supplier test scenarios will be aligned to business processes ▪ SMDA scenarios not developed but planned	No defined testing order but reliability testing, MID and CE likely to be completed first and CPA last	▪ GFI tool will build early confidence in GBCS compliance ▪ Early availability of DCC end-to-end test environment seen as critical by most stakeholders ▪ The stability and clarity of SMETS/ CHTS/ GBCS and related IRPs

Figure 7: Summary of findings of recent stakeholder engagement on device assurance

© Crown copyright 2015
Department of Energy & Climate Change
3 Whitehall Place
London SW1A 2AW
www.gov.uk/decc
URN: 15D/419